New Jersey
Office of Counter-Terrorism

IAC Bulletin No. 22

Wednesday, May 14, 2003

Sidney J. Caspersen, Director

Current Alert Level

ELEVATED
Significant Risk of Terrorist Attacks

"FIZZER" WORM SPREADING

TO: ALL IAC SECTORS

A potentially harmful and stealthy Internet worm was discovered last week and is still spreading. The so-called "Fizzer" worm, which can spread via e-mail as well as over file-sharing networks, is more dangerous than similar worms because of its malicious payload. Specifically, Fizzer can cause confidential data to be leaked from infected computers. The worm installs a keyboard-logging program that intercepts and records all keyboard strokes in a separate file. To transmit this information, Fizzer loads a backdoor utility that allows hackers to remotely control the infected computer via IRC channels.

The worm spreads by locating Microsoft Outlook and Windows address books and uses records stored there to send copies out to those addresses. Fizzer also infects the shared filing folder used by the KazaA peer-to-peer file-sharing application and is capable of spreading over the KazaA network and through vulnerable shared directories.

In an attempt to foil detection, Fizzer attempts to shut down an array of widely used anti-virus programs that might be running on a victim's personal computer.

At bottom, Fizzer is a mass-mailing worm that arrives in users' mailboxes in an e-mail with a random subject line and text. According to the Symantec Corporation, the following are subject lines randomly chosen from a list carried by the worm:

- **I thought this was interesting**
- **Rather psychedelic**
- **Found this on the net, you might like . . . .**
- **Discothèque**
- **Imbrue**
- **Damn it feels good to be gangsta [sic]**
- **The way I feel – Remy Shand**
- **Paradigm Shift**
- **WASSUP!**
- **Know Thyself**
- **Hell**
- **I love you**
- **Please discard if you don't like or agree with out leadership**
- **Little popup remover**
- **B Cannot Remember**
- **Yo, Wassup, B?**
- **An interesting program . . . .**
- **You might not appreciate this . . . .**
- **I think you might find this amusing . . . .**
- **LOL**
- **Check this out . . . hehehe**
- **Question . . . .**
- **See you tomorrow**
- **How are you?**
- **Why?**
- **Kind of simple, but fun nonetheless**
- **Check it out**

To avoid infections, users are advised to apply standard precautions. Do not open unsolicited attachments, even when they come from frequent contacts, and update anti-virus tools to detect the worm. Corporate anti-virus vendors such as McAfee and Symantec are currently updating signature definitions to

recognize Fizzer. Although it is possible to remove the worm from an infected system, prevention is the key.

If you suspect that you have been the victim of the Fizzer worm, please report the incident to the Computer Analysis and Technology Unit (CATU) of the New Jersey Division of Criminal Justice at that unit's 24-hour tips number, (800) 396-2310, or by using CATU's Cyber Threat/Intrusion Online Form at http://www.state.nj.us/lps/dcj/catu/catunit.htm. The High Technology Crimes & Investigative Support Unit of the New Jersey Police can also be contacted at (609) 882-2000.

As always, all suspicious activities should be reported to the New Jersey Office of Counter-Terrorism at (609) 341-3100 and your local police.

Any questions regarding preventative measures related to this advisory should be addressed to Assistant Director Cherrie M. Black or Deputy Attorneys General Allen Ferg and Ben Barlyn at (609) 341-2970.